Nations Unies A/CN.9/WG.IV/WP.158

Assemblée générale

Distr. limitée
1er février 2019
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-huitième session
New York, 8-12 avril 2019

Remarques explicatives sur le projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance

Note du Secrétariat

Table des matières

V.19-00603 (F)

I. Introduction

1. La présente note fournit des remarques concernant le projet de dispositions relatives à la reconnaissance internationale de la gestion de l'identité et des services de confiance qui figure dans le document A/CN.9/WG.IV/WP.157. Un historique des travaux du Groupe de travail sur les questions juridiques liées à la gestion de l'identité et aux services de confiance est par ailleurs présenté dans le document de travail A/CN.9/WG.IV/WP.156 (par. 6 à 15).

II. Objectifs généraux essentiels du projet de dispositions

2. Au cours des 20 dernières années, les activités en ligne ont connu une croissance exponentielle. La progression des activités commerciales en ligne (c'est-à-dire des opérations électroniques entre entreprises, entre entreprises et consommateurs, et entre entreprises et États) est particulièrement importante en valeur. De 64 millions de dollars en 1999, le commerce électronique mondial est ainsi passé à plus de 25 000 milliards de dollars en 2015[1], croissance qui coïncide avec celle de l'accès à Internet pour les particuliers et les entreprises. Par exemple, la part des ménages ayant accès à Internet est passée de 35 % en 2002 à 83,6 % en 2017[2]. La disponibilité de services numériques publics (y compris des services à caractère commercial), bancaires et de paiement a augmenté dans les mêmes proportions.

3. Cette croissance doit pouvoir s'appuyer sur un sentiment de confiance dans l'environnement en ligne. La capacité à identifier chaque partie de manière fiable, surtout en l'absence de toute interaction personnelle préalable, constitue l'un des aspects importants de la confiance en ligne. Au fil des années, diverses solutions ont été proposées pour répondre au besoin d'identification en ligne, ce qui a conduit à la multiplication des méthodes, des technologies et des dispositifs destinés à la gestion de l'identité. Le traitement au niveau mondial des aspects juridiques de la gestion de l'identité peut permettre non seulement de relier ces différentes solutions, mais aussi de favoriser l'interopérabilité des systèmes de gestion de l'identité, qu'ils soient exploités par des opérateurs privés ou publics.

4. Le développement du recours à la gestion de l'identité et aux services de confiance se heurte à plusieurs obstacles, dont certains de nature juridique, à savoir : 1) l'absence de législation donnant des effets de droit à la gestion de l'identité et aux services de confiance ; 2) l'existence de lois et d'approches divergentes en matière de gestion de l'identité, notamment de lois fondées sur des exigences spécifiques à une technologie ; 3) l'application de lois exigeant des documents d'identité papier pour la conclusion d'opérations commerciales en ligne ; et 4) l'absence de mécanismes pour la reconnaissance juridique internationale de la gestion de l'identité et des services de confiance (A/CN.9/965, par. 52).

5. Le principal objectif du Groupe de travail est de surmonter ces obstacles en élaborant des règles juridiques uniformes. Ces règles ont plusieurs objectifs : accroître l'efficacité ; abaisser les coûts des opérations ; augmenter la sécurité des opérations électroniques, notamment la sécurité juridique, de manière à instaurer la confiance ; et réduire la fracture numérique.

6. Ce faisant, le Groupe de travail contribuera à la réalisation des objectifs de développement durable. Plus précisément, l'importance de l'identité est soulignée dans l'objectif de développement durable n° 16, dont la cible 9 consiste à garantir à

[1] Source : CNUCED, Rapport 2001 sur le commerce électronique et le développement, document des Nations Unies, UNCTAD/SDTE/ECB/1, p. 44 (disponible en anglais seulement) ; CNUCED, Rapport sur l'économie de l'information 2017, document des Nations Unies, UNCTAD/IER/2017, p. 34.

[2] Source : UIT, Statistiques sur les TIC, Évolution des TIC à l'échelle mondiale, 2001-2018, disponible (en anglais seulement) à l'adresse https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

tous une identité juridique, ce qui, dans le contexte de l'économie numérique, correspond au droit à une identité numérique. L'établissement d'un cadre juridique pour la gestion de l'identité et les services de confiance aidera à rendre l'identité numérique opérationnelle en toute sécurité. En favorisant la confiance dans l'environnement en ligne, ce cadre contribuera également au développement durable et à l'inclusion sociale, conformément à l'objectif de développement durable n° 9, qui vise, entre autres, à encourager l'innovation.

III. Remarques explicatives sur le projet de dispositions

A. Chapitre I. Champ d'application (projets d'articles 1 à 3)

1. Objet de l'utilisation de systèmes de gestion de l'identité (projet d'article 1-1)

7. L'identification peut être nécessaire à différentes fins, à savoir pour veiller au respect des règlements, établir la validité d'un document commercial et satisfaire aux obligations contractuelles (A/CN.9/965, par. 82 et 83 ; voir également A/CN.9/WG.IV/WP.153, par. 32 à 34). **Le Groupe de travail voudra peut-être se demander comment le projet de dispositions s'appliquerait aux fins du respect des règlements**.

2. Reconnaissance juridique internationale et interne (projet d'article 1-1)

8. L'existence d'un cadre juridique interne facilite la reconnaissance des systèmes de gestion de l'identité et des services de confiance étrangers, en établissant des notions juridiques utiles pour le mécanisme de reconnaissance. La reconnaissance internationale se trouve encore facilitée lorsque les législations internes comportent des règles harmonisées fondées sur des principes généraux communs, voire des dispositions identiques. Par ailleurs, la reconnaissance internationale de la gestion de l'identité, d'une part, et la reconnaissance entre systèmes de gestion de l'identité, indépendamment de tout élément d'extranéité, d'autre part, présentent une certaine similitude. C'est pourquoi le projet de dispositions a été élaboré en vue d'offrir une base tant pour un accord international que pour une législation type à adopter au niveau interne.

3. Entités concernées (projets d'articles 1-2 et 1-3)

a) Entités publiques

9. Si les travaux du Groupe de travail concernent avant tout les opérations entre entreprises, les systèmes de gestion de l'identité établis dans d'autres contextes liés aux opérations commerciales – notamment dans le contexte des services publics à caractère commercial, tels que les guichets uniques pour les opérations douanières – devraient également être pris en compte (A/CN.9/965, par. 83). Il est donc justifié d'inclure les entités publiques parmi celles auxquelles le projet de disposition est susceptible de s'appliquer.

10. **Le Groupe de travail voudra peut-être se demander si la participation des entités publiques aux opérations de gestion de l'identité ou aux services de confiance soulève des questions particulières**, en gardant à l'esprit l'application des principes de la neutralité technologique (voir ci-dessous, par. 23) et de l'autonomie des parties (voir ci-dessous, par. 24).

b) Identification des objets

11. Il a été estimé que les travaux du Groupe de travail devraient faciliter l'identification fiable tant des sujets (c'est-à-dire des personnes physiques et morales) que des objets (c'est-à-dire des objets physiques et numériques) des opérations, et que l'identification d'un objet pouvait être utile pour identifier les sujets d'une opération. En tout état de cause, il convient de maintenir une distinction claire entre sujets et

objets, étant donné que ces derniers n'ont pas de personnalité juridique et ne peuvent assumer de responsabilité (A/CN.9/965, par. 11).

12. Au paragraphe 3, la référence à la « vérification de l'identité » reflète la décision qu'a prise le Groupe de travail de concentrer ses travaux sur l'identité de transaction et, dans ce contexte, sur les questions liées à la reconnaissance, c'est-à-dire à la vérification de l'identité plutôt qu'à son attribution (A/CN.9/965, par. 10). L'identité de transaction (ou secondaire) et l'identité fondamentale (ou primaire) sont décrites plus en détail dans le document A/CN.9/WG.IV/WP.153 (par. 7 à 10).

4. Absence de nouvelle obligation d'identification (projet d'article 2-1)

13. Un principe général commun aux textes de la CNUDCI sur le commerce électronique réside dans le fait que le droit matériel, c'est-à-dire le droit applicable aux opérations commerciales en général, n'est pas touché.

14. Dans le contexte de la gestion de l'identité et des services de confiance, ce principe signifie que la législation relative à la gestion de l'identité n'introduit aucune nouvelle obligation d'identification, que la législation relative aux services de confiance n'introduit aucune nouvelle obligation d'utiliser un type particulier de services de confiance, et que les obligations existantes demeurent inchangées.

15. Il a été dit qu'il existait un lien étroit entre le principe de l'absence de nouvelle obligation d'identification et celui de l'autonomie des parties (A/CN.9/965, par. 110). On a aussi noté que de nouvelles obligations d'identification pourraient survenir du fait de l'utilisation d'un service de confiance particulier, mais que, en tout état de cause, l'utilisation de ce service se ferait sur une base volontaire (ibid.).

5. Référence aux lois relatives au respect de la vie privée et à la protection des données (projet d'article 2-2)

16. Le Groupe de travail a souligné l'importance que revêtaient les régimes de protection des données pour la gestion de l'identité et les services de confiance. Le projet d'article 2-2 comporte une référence expresse aux lois relatives au respect de la vie privée et à la protection des données, ce qui traduit l'importance accordée à ces lois par le Groupe de travail.

B. Chapitre II. Dispositions générales (projets d'articles 4 à 7)

1. Définitions (projet d'article 4)

17. Les projets de définitions figurant au projet d'article 4 ont été élaborés sur la base de la terminologie utilisée dans les textes existants de la CNUDCI sur le commerce électronique.

18. À sa cinquante-septième session, le Groupe de travail a prié le Secrétariat d'inclure dans la liste des définitions essentielles, à des fins de référence, plusieurs définitions tirées de l'article 3 du Règlement eIDAS[3]. Ces définitions sont les suivantes :

a) Par « identification électronique », on entend le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ;

b) Par « moyen d'identification électronique », on entend un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne ;

[3] Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

c) Par « données d'identification personnelle », on entend un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ;

d) Par « schéma d'identification électronique », on entend un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales ;

e) Par « authentification », on entend un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique ;

f) Par « source faisant autorité », on entend toute source, quelle que soit sa forme, à laquelle on peut se fier pour obtenir des données, des informations et/ou des éléments d'identification exacts pouvant être utilisés pour prouver l'identité ;

g) Par « partie utilisatrice », on entend une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance.

19. **Le Groupe de travail voudra peut-être se demander si ces définitions, qui ne correspondent pas aux termes définis par la CNUDCI, devraient remplacer ou compléter les définitions figurant au projet d'article 4**.

2. Principes généraux et interprétation uniforme (projets d'articles 5 à 7)

20. Les textes de la CNUDCI comportent généralement une disposition qui fait référence à leur origine uniforme et énonce une obligation d'interprétation uniforme. Le paragraphe 2 de l'article 5 a pour objet d'assurer le maintien de l'uniformité lors de l'interprétation et de l'application du texte législatif.

21. Le Groupe de travail a recensé les principes généraux suivants comme étant pertinents pour ses travaux sur les aspects juridiques de la gestion de l'identité et des services de confiance : 1) non-discrimination à l'égard de l'utilisation de moyens électroniques ; 2) équivalence fonctionnelle ; 3) neutralité technologique ; et 4) autonomie des parties (A/CN.9/936, par. 67).

22. Si ces principes généraux ont été élaborés dans le cadre des textes existants de la CNUDCI sur le commerce électronique afin d'être appliqués au niveau interne (voir, par exemple, les articles 3, 5 et 6 de la Loi type sur les signatures électroniques[4] (LTSE)), ils s'appliquent également au niveau international, en posant un fondement juridique interne qui permet au pays requis d'octroyer un statut juridique durable aux systèmes de gestion de l'identité et aux services de confiance étrangers.

23. L'importance du principe de neutralité technologique pour la gestion de l'identité a été pleinement reconnue. S'agissant des pays en développement, il a été dit que l'application de ce principe pourrait empêcher l'adoption de prescriptions techniques trop coûteuses ou trop complexes du point de vue des commerçants (A/CN.9/965, par. 38). En vertu de ce même principe, dans le contexte de la gestion de l'identité, il pourrait être nécessaire que la configuration minimale requise fasse référence aux propriétés du système, et non à des technologies spécifiques (A/CN.9/936, par. 69).

24. L'autonomie des parties est un principe fondamental du droit commercial. Toutefois, son application est soumise à des limitations énoncées dans les lois impératives (A/CN.9/936, par. 72). Ces limitations sont particulièrement importantes, car les exigences législatives satisfaites par l'utilisation des systèmes de gestion de l'identité et des services de confiance sont souvent impératives. À mesure de l'avancée de ses travaux, **le Groupe de travail voudra peut-être identifier les règles fondamentales que les parties ne pourraient modifier et auxquelles elles ne pourraient déroger, afin d'augmenter la sécurité et la prévisibilité de la**

[4] *Loi type de la CNUDCI sur les signatures électroniques* (publication des Nations Unies, numéro de vente : F.02.V.8).

reconnaissance internationale de la gestion de l'identité et des services de confiance (A/CN.9/965, par. 109). En conséquence, il n'a pas été élaboré de projet de disposition sur l'autonomie des parties (sur la base, par exemple, de l'article 5 de la LTSE). Toutefois, des éléments du principe de l'autonomie des parties sont inclus dans le projet d'article 3.

25. Le principe de l'autonomie des parties vise également à appuyer l'exécution des accords contractuels, tels que les règles de fonctionnement relatives à la gestion de l'identité et les règles de fonctionnement et cadres relatifs aux services de confiance. Les règles de fonctionnement pourraient être particulièrement importantes dans le contexte des fédérations de systèmes de gestion de l'identité (voir A/CN.9/WG.IV/WP.154, par. 39).

C. Chapitre III. Gestion de l'identité (projets d'articles 8 à 13)

1. Reconnaissance juridique de la gestion de l'identité sur la base de l'équivalence fonctionnelle (projet d'article 8)

26. Le principe de l'équivalence fonctionnelle fait appel à une définition des exigences auxquelles un document, une méthode ou un processus électronique doit satisfaire pour remplir les mêmes fonctions que son équivalent papier. Il a été dit qu'une disposition sur l'équivalence fonctionnelle ne s'appliquerait que dans la mesure où l'identification au moyen d'un support papier serait pertinente (A/CN.9/965, par. 69), et qu'il faudrait peut-être, le cas échéant, formuler dans la disposition un lien avec les processus de gestion de l'identité hors ligne (A/CN.9/965, par. 66).

27. À sa cinquante-septième session, le Groupe de travail a mis en avant certains éléments à inclure dans une disposition sur l'équivalence fonctionnelle qui donnerait des effets juridiques à la gestion de l'identité : une référence à un élément d'identification physique utilisé dans l'environnement hors ligne (qu'il s'agisse d'un document, d'un registre ou d'une autre source faisant autorité) ; une référence à toutes les étapes du processus de gestion de l'identité (par exemple, l'identification et l'authentification) ; et une référence aux niveaux de garantie ou à un autre critère pour l'évaluation de la confiance dans l'exactitude de l'identification (A/CN.9/965, par. 70 à 78).

28. Des avis divergents ont été exprimés au sein du Groupe de travail quant à l'objet de la reconnaissance juridique (A/CN.9/965, par. 25), qui lui-même déterminerait l'orientation d'une éventuelle disposition sur l'équivalence fonctionnelle. Dans le contexte de la gestion de l'identité, l'objet de la reconnaissance juridique peut être : a) le système de gestion de l'identité ; b) les justificatifs d'identité délivrés par un système de gestion de l'identité ; ou c) les résultats du processus d'identification mené à l'aide d'un système de gestion de l'identité (c'est-à-dire l'identité de transaction) (A/CN.9/965, par. 24).

29. Selon l'avis qui a prévalu, le Groupe de travail devait se concentrer sur la reconnaissance des processus (c'est-à-dire des systèmes) et des résultats, tant pour ce qui était de la gestion de l'identité que des services de confiance (A/CN.9/965, par. 94 à 99). À cet égard, on a indiqué la complémentarité de la reconnaissance juridique des systèmes de gestion de l'identité, des justificatifs et des résultats du processus d'identification (A/CN.9/965, par. 26). En conséquence, si les systèmes de gestion de l'identité sont reconnus, alors les justificatifs utilisés pour l'identification le sont également, de même que les résultats du processus d'identification. Les deux variantes du projet d'article 8, qui ont été examinées à la cinquante-septième session du Groupe de travail, reflètent cette approche.

30. Dans certains cas, il se pourrait que l'identification soit menée uniquement en ligne et que l'équivalence fonctionnelle n'ait pas lieu de s'appliquer (A/CN.9/965, par. 62). Afin de traiter l'ensemble des cas, il a été proposé que le Groupe de travail examine les caractéristiques d'une méthode d'identification acceptable, plutôt que

d'essayer d'élaborer des dispositions sur l'équivalence fonctionnelle (A/CN.9/965, par. 69).

2. Normes de fiabilité (projet d'article 9)

31. Dans une disposition sur l'équivalence fonctionnelle, les éléments à prendre en compte pour la détermination de la fiabilité de la méthode comprennent : a) les accords contractuels, s'ils sont autorisés par la loi applicable ; b) la certification et la supervision ; et c) les niveaux de garantie.

a) Certification

32. Leur certification peut grandement contribuer à instaurer la confiance dans les prestataires de services de gestion de l'identité et de services de confiance, ainsi que dans leurs services. Les options de certification comprennent : l'autocertification, la certification par un tiers indépendant ; la certification par un tiers indépendant accrédité ; et la certification par un organisme public. Le type de service en jeu, le coût et le niveau de confiance requis influent sur le choix de la forme de certification la plus appropriée. Dans le contexte interentreprises, il convient d'offrir toutes les options de certification, y compris l'absence de certification, dans la mesure où les partenaires commerciaux devraient être en mesure de choisir la solution la mieux adaptée à leurs besoins, étant entendu que chaque option aurait des effets juridiques différents (A/CN.9/965, par. 112).

33. Toutefois, il a été estimé que toute solution présupposant l'intervention d'un organisme central de certification, d'accréditation ou de supervision pourrait ne pas convenir lorsque la technologie du registre distribué était utilisée, en raison des difficultés à identifier l'organisme qualifié pour demander la certification et celui chargé de l'évaluation, et à prendre des mesures correctives et coercitives, entre autres (A/CN.9/965, par. 114 et 129).

34. Dans les mécanismes de reconnaissance juridique existants (voir A/CN.9/WG.IV/WP.153, par. 61 à 73 et 76 à 79) fondés sur une approche *ex ante* (voir ci-dessous, par. 47 à 49), la certification (y compris l'autocertification) est un élément nécessaire à l'évaluation des systèmes de gestion de l'identité utilisant des normes axées sur les résultats.

35. La certification peut également être pertinente pour la reconnaissance juridique *ex post* (voir ci-dessous, par. 44 et 45). Par exemple, les alinéas e) et f) de l'article 10 de la LTSE mentionnent, sans toutefois rendre ces éléments obligatoires, l'existence de l'accréditation, des audits et de l'autocertification en tant que facteurs pouvant être pris en compte pour évaluer la fiabilité des systèmes utilisés par un prestataire de services de certification.

36. Des avis divergents ont été exprimés quant à l'opportunité de faire intervenir les pouvoirs publics dans le processus de certification. D'une part, il a été dit que la certification volontaire n'impliquait pas nécessairement l'intervention d'entités publiques et qu'elle pouvait reposer sur un mécanisme indépendant (A/CN.9/965, par. 112).

37. D'autre part, il a été indiqué que le contrôle exercé par l'État sur les activités des organismes de certification du secteur privé était essentiel pour prévenir les risques en matière de concurrence et les abus, en particulier en ce qui concernait les petits acteurs du marché (A/CN.9/965, par. 115 et 128). Par ailleurs, il a été dit que l'accréditation par les pouvoirs publics visait à faire en sorte que les organismes de certification conduisent leurs activités avec indépendance, impartialité et équité. À cet égard, on a estimé qu'une autorité indépendante serait peut-être mieux à même d'atteindre ces objectifs (A/CN.9/965, par. 115).

38. L'approche suivie à l'article 10 de la LTSE découle du principe de neutralité. L'incorporation de dispositions impératives sur la supervision peut se voir comme empêchant l'adoption d'un modèle de marché fondé sur l'autoréglementation des services de confiance.

b) Supervision

39. La supervision des systèmes de gestion de l'identité est courante, car son existence est jugée utile, voire nécessaire, à l'instauration de la confiance dans les prestataires de services et dans les services qu'ils fournissent. Toutefois, la mise en place d'un organe de supervision a des répercussions administratives et financières. Certains mécanismes complémentaires ou de substitution (comme la certification par des tiers) peuvent aider à atteindre les objectifs visés par la supervision, tout en réduisant les coûts associés.

40. Il a été dit que les pouvoirs publics jouaient un rôle croissant non seulement dans la supervision, mais aussi dans l'élaboration et le déploiement des systèmes de gestion de l'identité et dans la fourniture de services de gestion de l'identité et de services de confiance, et qu'il était nécessaire, dans ce contexte, de séparer leurs fonctions de supervision des autres fonctions qu'ils exerçaient (A/CN.9/965, par. 128).

c) Niveaux de garantie et mise en correspondance

41. Le niveau de garantie est une mesure du degré de confiance dans l'identification et les processus d'authentification, d'où son caractère essentiel dans l'établissement de la fiabilité d'un système de gestion de l'identité (A/CN.9/965, par. 61). Des avis divergents ont été exprimés quant à l'opportunité de faire référence aux niveaux de garantie (voir A/CN.9/965, par. 63 à 68).

42. Il pourrait être fait référence aux niveaux de garantie dans une disposition sur l'équivalence fonctionnelle (projet d'article 8) ou dans une disposition qui établirait des normes concernant la fiabilité du système de gestion de l'identité (projet d'article 9). **Le Groupe de travail voudra peut-être se demander, dans le cas où il serait fait référence aux niveaux de garantie, si une référence générique suffirait, ou s'il serait nécessaire de faire référence à différents niveaux de garantie** et, dans le second cas, si chaque niveau de garantie devrait être associé à un effet juridique distinct (voir A/CN.9/965, par. 59 et 60).

43. À sa cinquante-septième session, le Groupe de travail a examiné la méthode de « mappage » (mise en correspondance) servant à vérifier si un système de gestion de l'identité était conforme à la description générique d'un niveau de garantie (voir A/CN.9/965, par. 43 à 48 et 54). Un exemple pratique illustrant la manière dont ce processus pourrait fonctionner est présenté dans le document A/CN.9/WG.IV/WP.153 (par. 80).

3. Détermination *ex post* de la fiabilité (projet d'article 9)

44. Le projet d'article 9 vise à mettre en œuvre une approche *ex post* pour la détermination de la fiabilité des systèmes de gestion de l'identité. Cette approche consiste à ne procéder à l'évaluation d'un système de gestion de l'identité qu'en cas de survenue d'un litige, sur la base, toutefois, de conditions prédéfinies. Elle a été suivie dans les textes de la CNUDCI en ce qui concerne les services de confiance (voir, par exemple, l'article 9-3 de la Convention sur les communications électroniques).

45. On trouvera des informations supplémentaires sur l'approche *ex post* dans les documents A/CN.9/965 (par. 40 à 45) et A/CN.9/WG.IV/WP.153 (par. 74 et 75).

4. Présomption de fiabilité (projet d'article 10)

46. Le projet d'article 10 est basé sur l'article 6-3 de la LTSE, en vertu duquel les signatures électroniques qui satisfont à certaines exigences bénéficient d'une présomption de fiabilité. Il peut faire l'objet à la fois d'une application *ex post* et *ex ante*. Dans le cadre de l'approche *ex post*, il facilite l'application du projet d'article 9, en formulant des critères techniques objectifs qui aident à déterminer la fiabilité. Toutefois, ces mêmes critères peuvent être évalués *ex ante* par un organe

spécifique, le projet d'article 10 s'appliquant alors conjointement avec le projet d'article 11.

5. Détermination *ex ante* de la fiabilité (projet d'article 11)

47. Le projet d'article 11 vise à mettre en œuvre une approche *ex ante* pour la détermination de la fiabilité des systèmes de gestion de l'identité.

48. Cette approche présuppose la définition préalable des conditions qu'un système de gestion de l'identité doit satisfaire pour figurer sur une liste blanche de systèmes reconnus. L'avis a été exprimé que l'approche *ex ante* était préférable lors de l'utilisation de niveaux de garantie supérieurs (A/CN.9/965, par. 47).

49. Lors des délibérations du Groupe de travail concernant cette approche, deux points ont été soulevés : 1) la nécessité de mettre en place un mécanisme institutionnel centralisé pour l'évaluation des systèmes de gestion de l'identité ; et 2) la participation des pouvoirs publics. On trouvera des informations supplémentaires sur les mécanismes institutionnels à utiliser pour mettre en œuvre l'approche *ex ante* dans les documents A/CN.9/965 (par. 40 à 45) et A/CN.9/WG.IV/WP.153 (par. 61 à 73). Des informations supplémentaires sur la participation des pouvoirs publics figurent dans le document A/CN.9/965 (par. 49 et 50).

6. Obligations incombant aux opérateurs de systèmes de gestion de l'identité (projet d'article 12)

50. Le projet d'article 12-1 fournit de premiers éléments pour la définition des obligations fondamentales des opérateurs de systèmes de gestion de l'identité. Il est inspiré des dispositions correspondantes du Règlement eIDAS.

a) Obligation de notification des atteintes à la sécurité

51. Le projet d'article 12-2 établit l'obligation de notifier les atteintes à la sécurité. Cette obligation constitue un aspect du principe de transparence (A/CN.9/936, par. 88).

52. Les atteintes à la sécurité peuvent nuire à la fois aux systèmes et aux opérations. Il a été considéré qu'un mécanisme approprié de notification de ces atteintes était important pour améliorer la qualité de fonctionnement des systèmes et augmenter le niveau de confiance dans les services de gestion de l'identité et les services de confiance (A/CN.9/965, par. 123).

53. Il existe des éléments communs, mais également de grandes différences, entre les notifications d'atteinte à la sécurité et celles de violation des données. Des exemples de dispositions législatives existantes prévoyant un régime de déclaration des atteintes à la sécurité sont présentés dans le document A/CN.9/WG.IV/WP.154 (par. 43 et 44).

b) Obligation de communication de l'offre de services

54. Le Groupe de travail a examiné l'obligation de communiquer l'offre de services lors de ses délibérations sur le principe de transparence (A/CN.9/965, par. 121). La transparence de l'offre de services est importante non seulement pour les utilisateurs (auxquels elle permet de faire un choix éclairé), mais aussi pour les concurrents et les autres entités concernées (pour surveiller la concurrence sur le marché, par exemple) (A/CN.9/965, par. 121). Dans son libellé actuel, le projet d'article 12-1 n'établit pas d'obligation autonome de communication de l'offre de services.

55. Les opérateurs de systèmes de gestion de l'identité participant à des systèmes fédérés ou obtenant d'une autre manière la certification de leurs services auraient à communiquer une quantité importante d'informations. Des obligations d'information minimales pourraient être établies pour d'autres fournisseurs. Par exemple, l'article 9-1 de la LTSE contient une liste d'informations que le prestataire de services de certification doit fournir à la partie utilisatrice.

7. Responsabilité des opérateurs de systèmes de gestion de l'identité (projet d'article 13)

56. Il a été dit que, dans la mesure où les travaux du Groupe de travail traitaient de règles applicables au niveau national, il était nécessaire d'aborder le partage de la responsabilité (A/CN.9/965, par. 116), étant donné que le régime de responsabilité applicable pouvait avoir une incidence importante sur la promotion de l'utilisation de systèmes de gestion de l'identité et de services de confiance à des fins à la fois commerciales et non commerciales.

57. À cet égard, le Groupe de travail a dressé la liste suivante de questions à examiner : l'identification des entités qui devraient être tenues responsables, compte tenu des régimes spéciaux de responsabilité applicables aux entités publiques ; la possibilité de limiter la responsabilité des parties qui respecteraient les exigences préétablies ; les mécanismes statutaires de limitation de la responsabilité (par exemple, la dispense ou l'inversion de la charge de la preuve) ; et les limitations contractuelles de la responsabilité (A/CN.9/936, par. 85). Le document A/CN.9/WG.IV/WP.154 (par. 23 à 30) décrit brièvement la législation existante relative à la responsabilité des opérateurs de systèmes de gestion de l'identité.

58. Le projet d'article 13-1 applique le principe général selon lequel les opérateurs de systèmes de gestion de l'identité devraient être tenus responsables des conséquences de tout manquement à l'obligation de fournir les services conformément aux conditions convenues ou à d'autres exigences prévues par la loi (A/CN.9/965, par. 117). Toutefois, dans certains cas, l'opérateur peut être difficile à identifier (lors de l'utilisation de la technologie du registre distribué, par exemple).

59. Selon le libellé actuel de cette disposition, une entité publique peut être tenue responsable lorsqu'elle agit en tant que prestataire de services. Différents profils de responsabilité pourraient entrer en jeu lorsque l'entité publique exerce des fonctions de supervision et délivre des justificatifs d'identité fondamentale.

60. Dans son libellé actuel, le projet d'article 13 attribue la responsabilité uniquement aux opérateurs de systèmes de gestion de l'identité. **Le Groupe de travail voudra peut-être se demander si les règles relatives à la responsabilité devraient également s'appliquer aux autres entités concernées** (les utilisateurs et les tiers qui se fient à l'identification, par exemple), ou si, selon une autre approche, il faudrait appliquer à ces dernières des règles générales en matière de responsabilité. Il voudra peut-être également se demander si, par souci de transparence, les utilisateurs et autres entités concernées devraient obligatoirement être informés du régime de responsabilité applicable.

61. Le projet d'article 13 fait référence à l'intentionnalité et à la négligence comme fondements de la responsabilité. Un examen des normes de diligence, traitant notamment de la négligence ordinaire, de la présomption de négligence et de la responsabilité objective, dans le contexte de la responsabilité des opérateurs d'infrastructures à clefs publiques, figure dans le document intitulé « Promouvoir la confiance dans le commerce électronique »[5].

62. **Le Groupe de travail voudra peut-être se demander s'il faudrait établir des règles supplémentaires concernant la charge de la preuve et la définition des dommages**, ou si, à l'inverse, ces domaines devraient être régis par le droit interne applicable.

63. Le projet d'article 13-2 restreint la responsabilité des opérateurs de systèmes de gestion de l'identité pour les dommages dus à une utilisation dépassant certaines limites communiquées par eux. Cette disposition complète l'obligation de communication de l'offre de services, qui constitue un aspect du principe de transparence. Le document « Promouvoir la confiance dans le commerce

[5] *Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques* (publication des Nations Unies, numéro de vente: F.09.V.4), par. 179 à 201.

électronique » examine la possibilité de limitation ou d'exonération contractuelles de responsabilité pour les opérateurs d'infrastructures à clefs publiques[6].

64. Le projet d'article 13-3 présente un mécanisme qui encourage les opérateurs de systèmes de gestion de l'identité à adopter certaines normes, en faisant de leur utilisation une condition de l'exemption de responsabilité. Selon une autre approche, cette disposition pourrait faire référence à l'utilisation de niveaux de garantie supérieurs.

65. Le projet d'article 13-3 est subordonné au projet d'article 13-4. Le critère de « négligence grave ou de faute intentionnelle » est employé dans la loi de l'État de Virginie sur la gestion de l'identité électronique (voir A/CN.9/WG.IV/WP.154, par. 29).

66. Les autres moyens de traiter les questions relatives à la responsabilité comprennent la mise en place d'un mécanisme fondé sur l'assurance, dans lequel l'assureur indemnise les dommages découlant de l'utilisation d'un système de gestion de l'identité. Un autre mécanisme prévoit le déblocage automatisé d'indemnités préétablies ou des pénalités déterminées si certaines conditions sont remplies.

D. Chapitre IV. Services de confiance (projets d'articles 14 à 18)

67. À titre préliminaire, **le Groupe de travail souhaitera peut-être s'interroger quant à savoir s'il devrait établir une liste non exhaustive se fondant sur une définition commune de la notion de « service de confiance », ou plutôt prévoir des règles communes applicables à tous les services de confiance et des règles spécifiques applicables à chacun d'entre eux**. Une liste non exhaustive de services de confiance pourrait inclure : les signatures électroniques ; les cachets électroniques ; les horodatages électroniques ; les services d'envoi recommandé électronique ; l'authentification de site Internet ; l'archivage électronique ; les services de séquestre électronique ; et les preuves de présence électroniques.

1. Reconnaissance juridique des services de confiance sur la base de l'équivalence fonctionnelle (projet d'article 14)

68. Afin d'élaborer une disposition appropriée sur l'équivalence fonctionnelle pour un service de confiance, il faut déterminer les fonctions particulières que ce service vise à remplir. Le projet d'article 14 comprend des dispositions de base sur l'équivalence fonctionnelle adaptées à chacun des services de confiance recensés. **Le Groupe de travail voudra peut-être se demander si une disposition sur l'équivalence fonctionnelle des services de confiance devrait prévoir : a) des normes de fiabilité générales ou particulières ; b) la présomption de fiabilité ; c) l'évaluation *ex ante* de la fiabilité ; et d) une clause de sauvegarde sur la non-répudiation**.

a) Signatures électroniques

69. Le projet d'article 14-1 traite des signatures électroniques, qui constituent une forme courante de service de confiance. Tous les textes de la CNUDCI sur le commerce électronique comprennent des dispositions concernant leur utilisation.

70. Certains types de signatures électroniques et d'autres services de confiance, par exemple les services d'archivage électronique, peuvent apporter l'assurance de l'intégrité du message de données. Dans les textes de la CNUDCI, le maintien de l'intégrité d'un message de données est nécessaire à l'établissement de l'équivalence fonctionnelle avec la notion d'« original » dans l'environnement papier. **Le Groupe de travail voudra peut-être se demander s'il faudrait traiter l'assurance de l'intégrité comme un service de confiance distinct**.

[6] Ibid., par. 202 à 210.

b) Cachets électroniques

71. Selon le Règlement eIDAS, les cachets électroniques servent à prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document (Règlement eIDAS, 59e considérant). En outre, « les cachets électroniques peuvent servir à authentifier tout bien numérique de ladite personne, tel un code logiciel ou des serveurs » (Règlement eIDAS, 65e considérant).

72. Les textes de la CNUDCI sur les services de confiance s'appliquent à la fois aux personnes physiques et aux personnes morales. Il a été proposé d'étendre aux objets physiques et numériques la portée des travaux en cours au sein du Groupe de travail, de manière à couvrir également les codes de logiciels ou les serveurs.

73. Selon l'article 8 de la Loi type de la CNUDCI sur le commerce électronique[7] (LTCE), l'intégrité est nécessaire à l'établissement de l'équivalence fonctionnelle avec la notion d'« original » dans l'environnement papier. Le paragraphe 3 de l'article 6 de la LTSE fait référence à la notion d'« intégrité » dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte.

74. Compte tenu de ce qui précède, **le Groupe de travail voudra peut-être se demander s'il faudrait traiter les cachets électroniques comme un service de confiance distinct**, ou s'ils peuvent être considérés comme un sous-ensemble des signatures électroniques.

c) Archivage électronique

75. Le projet d'article 14-3 traite des services d'archivage électronique, qui eux-mêmes se rapportent à la question de la conservation des documents électroniques. Celle-ci peut concerner des documents qui ont été produits dès l'origine sous forme électronique ou qui reproduisent des informations initialement émises sur papier. Les services d'archivage électronique peuvent également apporter une garantie pour ce qui est de l'intégrité des documents électroniques archivés et du moment de l'archivage.

76. L'archivage électronique a pour fonction d'assurer la sécurité juridique concernant la validité des documents électroniques archivés, en cas de litige et pour d'autres besoins. Il a été proposé que le mécanisme de reconnaissance juridique pour l'archivage électronique se limite à assurer la conformité avec les exigences juridiques du pays dans lequel les documents archivés devaient être utilisés (A/CN.9/965, par. 126). Dans le cas où le Groupe de travail souhaiterait envisager d'élaborer une disposition sur l'archivage électronique, il lui est proposé de baser ses délibérations sur l'article 10 de la LTCE, qui traite de la conservation des messages de données.

77. Par ailleurs, la loi peut exiger que les documents électroniques archivés puissent faire l'objet d'une migration, afin qu'il soit possible d'y avoir accès indépendamment des évolutions techniques. Cette condition peut être satisfaite par l'application du principe de neutralité technologique et des exigences d'équivalence fonctionnelle avec la notion d'« intégrité », c'est-à-dire que, lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée (art. 8-1 b) de la LTCE).

d) Autres services de confiance

78. Les horodatages électroniques, qui font l'objet du projet d'article 14-2, visent à fournir la preuve de la date et de l'heure auxquelles le cachet a été apposé aux données. Ils peuvent également servir à prouver l'intégrité des données auxquelles se rapportent cette date et cette heure.

---

[7] *Loi type de la CNUDCI sur le commerce électronique* (publication des Nations Unies, numéro de vente : F.99.V.4).

79. Les services d'envoi recommandé électronique, qui sont traités au projet d'article 14-4, visent à prouver l'envoi d'une communication électronique par l'expéditeur identifié et sa réception par le destinataire identifié. Ils peuvent également apporter la preuve de l'intégrité des données échangées et du moment de l'envoi et de la réception de ces données.

80. Le projet d'article 14-5 traite de l'authentification de site Internet. Selon le Règlement eIDAS, « les services d'authentification de site Internet sont un moyen permettant au visiteur d'un site Internet de s'assurer que celui-ci est tenu par une entité véritable et légitime » (Règlement eIDAS, 67e considérant). **Le Groupe de travail voudra peut-être se demander s'il faudrait traiter l'authentification de site Internet comme un service de confiance distinct**, ou si elle peut être considérée comme un sous-ensemble des signatures électroniques.

81. Le projet d'article 14-6 traite des services de séquestre, qui consistent à assurer la garde d'un bien et à le remettre à qui de droit une fois remplies les conditions énoncées dans la convention d'entiercement. Ces services sont utilisés dans le contexte du paiement de sommes d'argent et de la mise à disposition de codes sources de logiciels. Par exemple, le paiement du prix de marchandises peut être retardé jusqu'à ce que les acheteurs les aient reçues ; dans le même temps, le vendeur reçoit confirmation du fait que l'argent destiné au paiement est disponible et sera débloqué dès réception et acceptation des marchandises.

82. Les services de preuve de présence électronique servent à prouver qu'un sujet se trouvait à un endroit donné à des moments précis. Ce service de confiance a été examiné dans l'optique des testaments électroniques. Il peut également être utile pour les inscriptions en ligne et les services bancaires. **Le Groupe de travail voudra peut-être se demander s'il convient d'élaborer une disposition spécifique sur les services de preuve de présence électronique**.

2. Présomption de fiabilité des services de confiance (projet d'article 15)

83. La LTSE et plusieurs lois internes sur les signatures électroniques établissent une distinction entre les services de confiance selon leur niveau de fiabilité. Plus précisément, selon ces lois, les signatures électroniques qui satisfont à certaines exigences emportent des effets juridiques et sont par conséquent réputées offrir un niveau de fiabilité plus élevé. Afin d'éviter toute confusion, il est recommandé que les travaux du Groupe de travail fassent référence à des niveaux de fiabilité lors de l'examen des services de confiance, et que le terme « niveaux de garantie » ne soit utilisé que dans le contexte des systèmes de gestion de l'identité.

84. **Le Groupe de travail voudra peut-être se demander si la notion de niveaux de garantie devrait s'appliquer à la reconnaissance des services de confiance**, ou si une autre notion devrait s'appliquer pour établir la fiabilité d'un service de confiance particulier. Il a été dit que des justificatifs d'identité offrant un niveau de garantie élevé pourraient être utilisés pour des services de confiance présentant des niveaux de fiabilité différents (A/CN.9/965, par. 106). Ainsi, il n'y a pas de corrélation entre les niveaux de garantie de l'identification électronique et les niveaux de fiabilité des services de confiance.

3. Responsabilité des prestataires de services de confiance (projet d'article 18)

85. À titre de principe général, les prestataires de services de confiance devraient être tenus responsables des conséquences de tout manquement à l'obligation de fournir les services conformément aux conditions convenues ou à d'autres exigences prévues par la loi (A/CN.9/965, par. 117). Le type de service de confiance fourni déterminera l'étendue de cette responsabilité.

86. La LTSE comporte des dispositions traitant de la responsabilité liée au comportement du signataire (art. 8), du prestataire de services de certification (art. 9) et de la partie se fiant à la signature ou au certificat (art. 11). Ces dispositions précisent les obligations de chaque entité intervenant dans le cycle de vie de la

signature électronique. La LTSE prévoit en outre la possibilité que les prestataires de services de certification limitent la portée ou l'étendue de leur responsabilité.

87. Le document A/CN.9/WG.IV/WP.154 (par. 33 à 35) décrit brièvement la législation existante relative à la responsabilité des prestataires de services de confiance.

E. Chapitre V. Aspects internationaux (projets d'articles 19 et 20)

1. Reconnaissance juridique internationale (projet d'article 19)

88. La reconnaissance juridique internationale peut s'entendre de différentes façons (voir A/CN.9/WG.IV/WP.153, par. 55). À la cinquante-septième session du Groupe de travail, il a été dit que l'approche à privilégier en la matière était l'octroi d'un traitement national (A/CN.9/965, par. 30). Le projet d'article 19 a été élaboré en conséquence.

89. Le régime de responsabilité applicable peut jouer un rôle dans l'évaluation de l'équivalence d'un système de gestion de l'identité étranger. Il a donc été estimé que pour faciliter la reconnaissance internationale de la gestion de l'identité, il était nécessaire de déterminer le droit applicable au régime de responsabilité (A/CN.9/965, par. 116). Cela pourrait nécessiter l'élaboration d'une règle spécifique de droit international privé, ou une référence à des règles existantes de cette nature. **Le Groupe de travail voudra peut-être se demander si la reconnaissance juridique internationale impliquerait l'application du régime de responsabilité interne aux services de gestion de l'identité et aux services de confiance étrangers**.

90. Le projet d'article 19 n'aborde pas expressément la limitation de responsabilité. À cet égard, l'application de règles supplémentaires, relevant notamment de la loi impérative, pourrait restreindre la validité des clauses contractuelles.

91. Le projet d'article 19-2 prescrit le niveau de fiabilité comme critère d'évaluation de l'équivalence d'un système de gestion de l'identité ou de justificatifs de gestion de l'identité étrangers. Il présente deux variantes, selon que le système de gestion de l'identité étranger offre le même niveau de fiabilité ou un niveau de fiabilité substantiellement équivalent. La notion de « niveau de fiabilité substantiellement équivalent » est reprise de l'article 12 de la LTSE. **Le Groupe de travail voudra peut-être se demander si, en ce qui concerne la reconnaissance de la gestion de l'identité, il faudrait donner des orientations supplémentaires sur la référence à la notion de niveaux de garantie et sur l'utilisation de la mise en correspondance**.

2. Mécanismes de coopération institutionnelle (projet d'article 20)

92. Des mécanismes de coopération institutionnelle pourraient contribuer à assurer la reconnaissance juridique mutuelle et l'interopérabilité des systèmes de gestion de l'identité et des services de confiance.

93. Le projet d'article 20 aborde la coopération institutionnelle sous la forme de la coopération entre États. La coopération peut consister en des échanges d'informations, de données d'expérience et de bonnes pratiques, notamment en ce qui concerne les exigences techniques et les niveaux de garantie, l'évaluation par les pairs des systèmes d'identification électronique et l'examen des évolutions pertinentes. Un des actes d'exécution[8] du Règlement eIDAS fournit des détails supplémentaires sur l'échange d'informations et l'évaluation par les pairs, notamment en indiquant que l'État membre fournit les informations demandées sauf si leur communication risque de porter atteinte à la sécurité publique ou nationale, ou à des secrets commerciaux, professionnels ou industriels.

[8] Décision d'exécution (UE) 2015/296 de la Commission du 24 février 2015 établissant les modalités de coopération entre les États Membres en matière d'identification électronique.

94. La fédération des systèmes de gestion de l'identité pourrait permettre d'assurer une autre forme de coopération. En général, les fédérations reposent sur des accords contractuels, même si des dispositions législatives peuvent aider à promouvoir cette pratique. Pour plus d'informations sur la fédération des systèmes de gestion de l'identité, voir le document A/CN.9/WG.IV/WP.154 (par. 39).

95. Le fonctionnement des fédérations de systèmes de gestion de l'identité se fonde sur l'interopérabilité technique ainsi que sur un cadre juridique commun défini par un ensemble de règles systémiques. L'harmonisation des règles contractuelles et législatives peut favoriser la mise en place de ce cadre (A/CN.9/965, par. 120).

96. Il a été dit que l'adoption d'un mécanisme de reconnaissance juridique *ex ante* pourrait également déboucher sur une forme de coopération institutionnelle.